CHAPTER 1

INTRODUCTION

1.1 VIRTUAL PRIVATE NETWORKS

With the introduction of the computer, the need for automated tools for protecting files and other information stored in the computer became evident. This is especially the case for a shared system and the need is even more acute for systems that can be accessed over a public telephone network, data network or the Internet. Network security is the process of protection of networks and their services from unauthorized modification, destruction, or disclosure. The major change that affected security is the introduction of distributed systems and the use of networks and communication facilities for carrying the data between one computer and another. Network security controls are used to prevent the access of intruders in networks. Virtual Private Networks is one of the network security controls used to prevent the intruder to access the networks.

VPNs are used in three internetworking scenarios. The "Intranet" VPN exists between the corporation and its branch offices. The "Remote-access" VPN is used for communication between the corporation and mobile or remote employees. Finally, the "Extranet" VPN is used between the corporation and its business partners or associations (Figure 1.1).
1.1.1 Intranet VPNs

An intranet VPN is created between the corporate headquarters and a remote sales office, or between headquarters and remote satellite offices. The only difference here is that the intranet is accessed outside the network, meaning the access to it comes from the outside. Typically, it is only used inside a company’s network and accessed by company employees. An intranet VPN is still accessed by the company employees, but the access comes from outside rather than inside. This type of VPN is much more complex and less secure than other implementations.

1.1.2 Remote-Access VPNs

With remote access VPNs the burden of companies having to manage large modem banks is eliminated. Using the Internet for remote
access is much easier and more cost-effective than the traditional dial-in lines. The basic procedure in this scenario is that the remote user dials into his or her nearest ISP through which the connection is tunneled into the corporate network. The remote clients, however, do not have to deal with the responsibility of managing their own network. Remote access VPNs can give detailed information about the user to facilitate access control. The network administrators can set up detailed access control mechanisms to restrict the remote user to those resources that the user will require.

1.1.3 Extranet VPNs

The major concern in an extranet VPN solution is the versatility of the system. Extranet VPNs must be interoperable with respect to platforms, protocols, and authentication and encryption methods. Extranets are mainly used to connect business partners. In this respect, all aspects of communication must be secure. In particular, the aspect of confidentiality is now important. It is vital that the data does not lose its integrity in transit, and thus extranet VPNs must be the most secure VPNs. The usual structure of such systems is to have a VPN proxy server resident behind a firewall. In this way, any traffic that passes the firewall can be filtered by the VPN server according to the company security policy.

1.1.4 Benefits of Virtual Private Networks

The benefits of Virtual Private Networks are:

- Improved security
- Simplified network topology
- Global networking opportunities
- Extended geographic connectivity
- Improved productivity
- Provides telecommuter support
- Reduces transit time and transportation costs for remote users

1.2 HOSE AND PIPE MODELS

1.2.1 Pipe Model in Virtual Private Networks

In the pipe model the VPN customer specifies the load between every pair of nodes, and the customer specifies the QoS requirements between every pair of VPN nodes. Thus, the pipe model requires the customer to know the complete traffic matrix, that is, the load between every pair of nodes. The number of nodes per VPN is constantly increasing and the communication patterns between nodes are becoming increasingly complex. As a result, it is almost impossible to predict the traffic characteristics between pairs of nodes required by the pipe model (Figure 1.2).

![Figure 1.2 Pipe Model in Virtual Private Networks](image-url)
1.2.2 Hose Model in Virtual Private Networks

A more elegant method is called the hose model (Figure 1.3). In this model, VPN customers need only to specify two parameters for each node:

- Egress bandwidth requirement: the bandwidth for aggregate outgoing traffic from one node to all the other nodes.
- Ingress bandwidth requirement: the bandwidth for aggregate incoming traffic out of all the other nodes to this node.

![Figure 1.3 Hose Model in Virtual Private Networks](image)

1.2.3 Advantages of the Hose Model

- Better bandwidth utilization.
- Customers need to specify only the ingress and egress traffic in the VPN environment; so it is easy for specification.
- Traffic from a given site can be distributed smoothly over other VPN sites.
1.3 PROVISIONING IN VIRTUAL PRIVATE NETWORKS

1.3.1 Provisioning Overview

The term provisioning is the process of preparing and equipping the network so that it can provide services to its users. A VPN provisioning is the process that determines how to connect provider edge nodes to each other across the core network. A Virtual Provider Network site potentially requires a virtual link to all other sites in the same VPN. Each such virtual link is mapped from the source customer edge nodes to the destination customer edge over their adjacent provider edge nodes, resulting in full-mesh virtual topology. If more than one VPN require a virtual link over the same two provider edges, their virtual links can be multiplexed on to the same path, or tunnel, across the core network. Multiplexing will, in general, decrease the number of provisioned paths seen by the core network, and thus improve the scalability.

Provisioning techniques for network resource virtualization must be designed to satisfy two primary objectives. The first objective is to satisfy the performance requirements for each customer’s network traffic. The second objective is to maximize the overall resource utilization efficiency of the network.

1.3.2 Need for New Provisioning VPN Algorithm

To determine the resources that need to be provisioned for a given routing structure one needs to know whether the VPN resource sharing state is available in the network and have a specification of the VPN’s traffic. If the network supports the VPN specific state for resource sharing, then trees that traverse a common link can share a capacity reservation on that link. Such
sharing is particularly desirable when there are variations in the VPN’s traffic loads. The degree to which bandwidth is known, and the routing algorithm selected, impact the extent to which such resource sharing can be exploited. For example, if a detailed bandwidth reservation is available (or measured) at each link, and sharing is supported, then the resources might be appropriately provisioned to meet the aggregate VPN traffic demands on each link. By contrast if only hose descriptors are available, and no resource sharing is supported, provisioning is likely to be conservative and more costly.

1.3.3 Provisioning Structures for VPNs

The various provisioning structures for Virtual Private Networks are:

- Hierarchical provisioning model.
- Ingress/Egress Tree model.
- Sink Tree model.
- Mesh model.

1.3.3.1 Hierarchical Provisioning Model

This model reduces the number of paths visible in the core network, in contrast with the other model traffic belonging to the different VPN, which can be multiplexed on to same path if appropriate. In this model, the provider edges are not directly connected with each other, but they are connected to intermediate cross connects in the network, that in turn, provide connectivity to other provider edges.
1.3.3.2 Ingress/Egress Tree Model

Every ingress of the VPN has a tree associated with it, that carries the traffic to all the egress points, and similarly, each egress of the VPN has a tree associated with it that carries traffic from all the ingress points. The tree might be provisioned, based on shortest paths, or some other VPN or node dependent metric.

1.3.3.3 Sink Tree Model

This model reduces the total amount of state information in the provider network. In the sink tree, the destination represents the route and multiple sources represent the leaves. The paths leading to every provider edge route forms a sink tree in the network, so the destination is regarded as sink.

1.3.3.4 Mesh Model

This model provides arbitrary routing by splitting the traffic flow between VPN nodes. A mesh reduces to a collection of individual pipes when splitting is not possible.

Normally, the request of provisioning would follow paths determined by the associated IP routing protocol. But the VPN dependent routing state may need to be maintained in the network. In reality, explicit routing would be required to support routing structures specifically engineered for a given VPN.
1.4 RESTORATION IN VIRTUAL PRIVATE NETWORKS

1.4.1 Network Recovery

If a failure occurs in a network, recovery is achieved by moving the traffic from the failed part of the network to another portion of the network. It is important that this recovery operation can be performed as fast as possible to prevent too many packets from getting dropped at the failure point.

Recovery techniques can be used in both circuit-switched and packet-switched networks. When a link or node in a network fails, the traffic that was using the failed component must change the path used to reach the destination. This is done by the routers adjacent to the failure; they update their forwarding tables to forward packets on a different path that avoids the failing component. The path that the traffic was using before the failure is called the primary path and the alternative new path is called the backup path.

Often recovery techniques consist of four steps. First, the network must be able to detect the failure. Second, nodes that detect the failure must notify certain nodes in the network of the failure. Third, a backup path must be computed. Fourth, instead of sending traffic on the primary path, a node called the Path Switching Node must send traffic on the backup path. This step is called switchover and completes the repair of the network after a failure.

In networks like the Internet, the recovery mechanisms rely on the capabilities of the routing protocols. If a failure occurs, each router in the network has to be informed about it and the routing tables in each router have to be recomputed using a shortest path first algorithm. When routing tables
have been recomputed and converted, all paths that were using a failed link or node are rerouted through other links.

Routing protocols use timers to detect when a failure has occurred. The routing protocol on a node periodically sends hello messages to its neighbor nodes. If a neighbor does not receive a preset number of hello messages in a time interval, then the routing protocol interprets this as a failure on the link to that node. When a network failure has been detected, all the nodes in the network have to be notified about the failure. Then each node has to perform a shortest path first calculation with the failed link pruned from the network. When all nodes have finished the calculation, new routing tables are updated and traffic can be rerouted in the network.

Routing protocols make the network able to survive one or multiple link or node failures, but they do not guarantee the recovery time. The recovery time strongly depends on the dimension of the network and on the routing protocol used.

The high availability of network connections is a key challenge to service providers to increase their revenue. When a path fails, the service provider must quickly re-establish another path so that the user can continue its VPN connectivity without interruption. Restoration mechanisms help in this regard.

1.4.2 Failure Modes

There are two different failure modes to protect against the failure of the link or node. The first is against link failures. The second is the node failures. The amount of resources needed to provide backup for the second mode will be greater since a node failure results in multiple link failures. In
In the link failure model, when a link fails, the two nodes that are at the end point of the link know that the link has failed and they immediately switch all the demands that go on this link to an alternative path. Note that when a node fails, the entire links incident on this node fail, and in this case, the backup path designed to protect against link failures may also fail. In the element failure model, a node fails to assume that all the link interfaces at that node fail, and therefore, all links that are incident on the node fail. This is detected as a link failure case and the demands are routed across the failed node. Note that in the case of element failures, there has to be a backup path for every node, instead of every link, traversed by the active path. It does not provide a backup if the source or the destination of the traffic fails.

1.5 THESIS CONTRIBUTIONS

The thesis contributions are:

- Designed and implemented a new algorithm called COVPA – Cost Optimized Virtual Private Networks Provisioning Algorithm for the VPN hose model with better performance than the Breadth First Search Algorithm, Steiner Tree Algorithm and Primal Dual Algorithm.

- Designed and implemented a new algorithm called KCDVT - K-Cost Optimized and Delay satisfied Virtual Private Networks Tree Provisioning Algorithm for the VPN hose model with better performance than the existing Breadth First Search Algorithm.

- Designed and implemented a new algorithm called ARA - Adjustment Restoration Virtual Private Networks Algorithm
for the VPN hose model providing better quality of service for the VPN than the existing Disjoint Path Algorithm.

- Designed and implemented a new algorithm called PRA - Provisioned Restorable Virtual Private Networks Algorithm for the VPN hose model, which provides better quality of service than both the provisioning algorithm and the restoration algorithm applied independently.

1.6 ORGANIZATION OF THE THESIS

The thesis is organized in the form of seven chapters.

Chapter 1 describes the basics of the Virtual Private Network and introduces the concepts of Hose and Pipe Models. This chapter also introduces Provisioning and Restoration algorithms in Virtual Private Networks. The thesis contributions are also given in chapter 1.

Chapter 2 provides a literature survey on algorithms in Virtual Private Networks. Various Provisioning Algorithms in Virtual Private Networks and providing quality of service guarantees in Provisioning of the VPN, are discussed. The application of scheduling in improving the Provisioning of the VPN is also presented. Various Restoration Algorithms and mechanisms to provide quality of service guarantees are also discussed. The motivation for carrying out this research and the objectives of the thesis too are presented.

Chapter 3 discusses about a Cost Optimized Virtual Private Networks Provisioning Algorithm. This chapter provides the modeling of a network backbone managed by service providers and introduces the Cost
Optimized Virtual Private Networks Provisioning Algorithm (COVPA). The simulation study results using the Waxman and Barabasi-Albert Model were presented. A performance analysis was conducted with a comparison of BFS and Steiner Tree routing. The effect of the number of network nodes, the number of VPN nodes and rejection ratio is presented.

Chapter 4 discusses a Provisioning Algorithm for the VPN in the hose model with quality of service support. This chapter presents the K-Cost Optimized and Delay Satisfied Virtual Private Networks Tree Provisioning Algorithm (KCDVT). A Simulation study using Waxman and Barabasi-Albert Model is presented. A performance analysis was carried out and a comparison of the present algorithm with the BFS algorithm is presented. The effect of the number of nodes, number of VPN nodes on cost and delay is also presented.

Chapter 5 discusses the Restoration algorithm in the VPN with quality of service paths. This chapter introduces various restoration models and quality of service constraints. The Adjustment Restoration Virtual Private Networks Algorithm (ARA) providing quality of service is presented. The results of the simulation study based on the Waxman and Barabasi-Albert Model is presented with a comparison with Disjoint Path Algorithm. The effect of number of nodes on cost and delay is presented.

Chapter 6 describes the Provisioning Restorable Virtual Private Networks Algorithm (PRA) for the Hose Model VPN to achieve better quality of service than independent Provisioning as well as the Restoration algorithm. This chapter describes the Restorable VPN and bandwidth sharing in the Restorable VPN. The concept of the Restorable VPN Provisioning Virtual Private Networks Algorithm is discussed. The results of the simulation study with Waxman and Barabasi-Albert Model is presented along with a
comparison with individual Restoration and Provisioning Algorithms. The results show that by combining Restoration and Provisioning, we are able to achieve better quality of service performance.

Chapter 7 provides the overall conclusion of the thesis. The summary of contributions is presented, and the conclusion mentions the advantages of the following algorithms 1. Cost Optimized Virtual Private Networks Provisioning Algorithm (COVPA) 2. K-Cost Optimized and Delay Satisfied Virtual Private Networks Tree Provisioning Algorithm (KCDVT) 3. Adjustment Restoration Virtual Private Networks Algorithm (ARA) and 4. Provisioning Restorable Virtual Private Networks Algorithm (PRA) over existing techniques. The improved performance of the proposed algorithm with lesser cost and lesser delay is presented.

The possible extensions of the present work including the use of additional models of network and achieving additional quality of service parameters are also discussed.